CLAIMS

1. A system with a local application entity and communications means by which the local application entity can exchange application messages with peer remote application entities on other systems, the communication means including a transport entity for providing transport services, and a security entity logically positioned above the transport entity and operative to set up secure communication sessions with peer security entities in other systems for the passing of application messages in protocol data units (PDUs) exchanged between the security entities, the security entity including a tunnelling mechanism for establishing a tunnel through an access-controlling intermediate system whereby to enable the local application entity to exchange application messages securely with a remote application entity on another system reachable via said intermediate system, the tunnelling mechanism establishing this tunnel by first setting up a first security session with said intermediate system and then a nested, second, security session with said another system with PDUs associated with the second session being encapsulated within PDUs associated with the first session and being extracted by the intermediate system for sending to said another system; and each PDU having a message-type field by which the security entity in the intermediate system can determine whether a PDU it receives encapsulates a PDU to be extracted and sent on.

2. A system according to claim1, wherein each PDU has a destination address which is modifiable without invalidating any security processing applied specifically to that PDU whereby the intermediate system can redirect PDUs that are indicated by the message type of an encapsulating PDU as intended for sending on.

3. A system according to claim 1, wherein each security session is between specified application entities and the establishment of a security session is effected through a handshake process between the security entities concerned during which each application entity involved is required to show, by attribute certificates exchanged between the security entities, that it possesses certain attributes required of it by the other application entity.

4. A system according to claim 3, wherein a remote broker system runs a broker application that fronts for a target application entity that the local application entity wishes to contact, the security entity of the local application entity being initially operative to seek to establish a security session with the broker application as said target application entity requiring of the broker application attributes considered by the local application entity as appropriate for the target application, the broker application responding by causing its associated security entity to return as part of its handshake with the security entity of said local application, an indication that the broker application is a relay for the target application entity, the local application entity being thereupon operative to decide whether to request a tunnel be set up through the broker system by the tunnelling mechanism and if so what attribute requirements must now be met by the broker application.

5. A system according to claim 1, wherein a remote broker system runs a broker application that fronts for a target application entity that the local application entity wishes to contact, the security entity of the local application entity being initially operative to seek to establish a security session with the broker application as said target application entity, the broker application responding by causing its associated security entity to return to the security entity of said local application, an indication that the broker application is a relay for the target application entity, the local application entity being thereupon operative to decide whether to request a tunnel be set up through the broker system by the tunnelling mechanism and if so what attribute requirements must be met by the broker application.

6. A system according to claim 1 wherein said tunnelling mechanism is capable of setting up multiply-nested security sessions for tunnelling through a corresponding number of intermediate systems.

7. A system with a local application entity and communications means by which the local application entity can exchange application messages with peer remote application entities on other systems, the communication means including a transport entity for

providing transport services, and a security entity logically positioned above the transport entity and operative to set up secure communication sessions with peer security entities in other systems for the passing of application messages in protocol data units (PDUs) exchanged between the security entities, each said security session being between specified application entities and the establishment of a security session being effected through a handshake process between the security entities concerned during which each application entity involved is required to show, by attribute certificates exchanged between the security entities, that it possesses certain attributes required of it by the other application entity; the security entity including a tunnelling mechanism for establishing a tunnel through an access-controlling intermediate system whereby to enable the local application entity to exchange application messages securely with a remote application entity on another system reachable via said intermediate system, the tunnelling mechanism establishing this tunnel by first setting up a first security session with said intermediate system and then a nested, second, security session with said another system with PDUs associated with the second session being encapsulated within PDUs associated with the first session and being extracted by the intermediate system for sending to said another system.

8. An arrangement comprising first, second and third systems each with a respective application entity and communications means by which the application entity can exchange application messages with the application entities on the other systems, the communication means including a transport entity for providing transport services, and a security entity logically positioned above the transport entity and operative to set up secure communication sessions with the security entities in the other systems for the passing of application messages in protocol data units (PDUs) exchanged between the security entities, the establishment of security sessions being dependent on each participating entity proving possession of, or access to, particular attributes, if any, required of it by the other entity; the security entity of the first system including a tunnelling mechanism for establishing a tunnel through the second system to the third system whereby to enable the application entity of the first system to exchange application messages securely with the application entity of the third system, the tunnelling mechanism establishing this tunnel by first setting up a first security session

with the second system and then a nested, second, security session through the second system to the third system with PDUs associated with the second session being encapsulated within PDUs associated with the first session and being extracted by the security entity of the second system for sending to the third system; the application entity of said second system being a broker application that fronts for a target application constituted by the application entity of the third system, the application entity of the first system on wishing to contact said target application causing its security entity to seek to establish a security session with the broker application as said target application, and the broker application being operative to respond by causing the security entity of the second system to return to the security entity of the first system, an indication that the broker application is a relay for the target application entity, the application entity of the first system being thereupon operative to request a tunnel be set up through the broker system by the tunnelling mechanism, the attributes required of the second system by the first system being potentially different when the second system is providing a tunnel rather than hosting the target application entity.